UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

S.R., individually and on behalf of all others similarly situated, Plaintiff, v. SATORI LASER CENTER CORP., Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff S.R. ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself, which are based on personal knowledge.

NATURE OF ACTION

1. This is a class action lawsuit brought against Defendant Satori Laser Center Corp. ("Defendant") on behalf of all persons who have visited the website satorilaser.com (the "Website") and booked an appointment for laser hair removal treatment.

2. When booking medical treatment online, patient privacy is crucial. Patients expect, as they should, that their private information will be held in confidence and not shared with third parties. The sensitive nature of information related to permanent hair removal treatment amplifies the need for privacy during online bookings, as these procedures often involve sensitive details of a patent's individual appearance and body image. Such information can be emotionally charged and stigmatizing, making the protection of such data critical.

3. Defendant owns and operates the Website, where patients can book laser hair removal treatments at one of its brick-and-mortar medical facilities. Defendant offers numerous

treatment options designating the specific part of the patient's body where the treatment will be performed, including, for example, the "areola," "buttocks," and "thong line."[1]

4. Unbeknownst to Plaintiff and members of the putative class, and contrary to Defendant's duties as a medical provider, Defendant discloses their individually identifiable health information to third parties, including Google, for targeted advertising purposes. Plaintiff brings this action for legal and equitable remedies resulting from Defendant's illegal actions.

THE PARTIES

5. At all relevant times, Plaintiff was a resident of Great Neck, New York. In or around November 2022, Plaintiff created an account on Defendant's Website to schedule appointments for laser hair removal treatment. On November 26, 2022, Plaintiff signed into her patient account and booked an appointment for laser hair removal treatment through Defendant's Website for Brazilian and Underarms laser hair removal treatment. Unbeknownst to Plaintiff, Defendant disclosed her personal information—as well as information related to the specific laser hair removal treatment she was seeking—to Google LLC ("Google") for targeted advertising purposes. After booking an appointment on Defendant's Website, Plaintiff began receiving targeted advertisements for similar products and services. Plaintiff would not have booked an appointment on Defendant's Website if she knew Defendant was violating her privacy by sharing her personal and medical information with unknown third parties.

6. Satori Laser Center Corp. is a New York corporation with its principal place of business in New York, New York. Defendant owns and operates a professional network of brick-and-mortar medical clinics that specialize in laser hair removal treatment. Laser hair

[1] https://www.satorilaser.com/collections/laser-hair-removal

removal treatment is a medical procedure.[2] Defendant also develops, owns, and operates the Website, which is used by consumers throughout New York and Pennsylvania to book appointments for laser hair removal treatment. Defendant chose to embed tracking technology on its Website, whereby it shared the confidential medical information of its patients with Google for targeted advertising purposes. Defendant did this without authorization or consent from its patients.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (the Electronic Communications Privacy Act, 18 U.S.C. § 2511). Further, this action is a putative class action, and Plaintiffs allege that at least 100 people comprise the proposed class, that the combined claims of the proposed class members exceed $5,000,000 exclusive of interest and costs, and that at least one member of the proposed class is a citizen of a state different from at least one defendant.

8. This Court has personal jurisdiction over Defendant because Defendant conducts substantial business within this District.

9. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to this claim occurred in this District.

FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS

A. Health-Related Information is Sensitive and Confidential

10. Defendant assisted Google, one of the largest technology companies in the world, with intercepting information that is sensitive, confidential, and personally identifiable.

[2] https://www.mayoclinic.org/tests-procedures/laser-hair-removal/about/pac-20394555

11. Defendant operates a network of laser hair removal medical clinics through New York and Pennsylvania. Defendant's operations are overseen by its Medical Director, Loretta Pratt, MD.[3]

12. Under federal law, a healthcare provider may not disclose personally identifiable information ("PII") or protected health information ("PHI") without the patient's express written authorization.[4] In this case, PHI includes but is not limited to information pertaining to laser hair removal appointments.

13. The United States Department of Health and Human Services ("HHS") has established a national standard, known as the HIPAA Privacy Rule, to explain the duties healthcare providers owe to their patients. "The Rule requires appropriate safeguards to protect the privacy of [PHI] and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization."[5]

14. A healthcare provider violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-d9 ("Part C"): "(1) uses of causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."[6]

15. The statute states that an entity "shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity…and the individual obtained or disclosed such information without authorization." *Id*.

---

[3] https://www.satorilaser.com/pages/medical-director?srsltid=AfmBOookBvf5eJPVA5czR9xEi52wk9v1JvDunFcuzQ1YVQbr0JD4Tbud

[4] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).

[5] U.S. Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[6] 42 U.S.C. § 1320d-6.

16. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to its patients.

17. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained and transmitted in violation of 45 C.F.R. Section 164.306(a)(1);

b. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.R.F. Section 164.308(a)(1);

c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendant in violation of 45 C.F.R. Section 164.308(a)(6)(ii);

d. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. Section 306(a)(2);

e. Failing to protect against reasonably anticipated uses of disclosures of electronic PHI not permitted under privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. Section 164.306(a)(3); and

f. Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably

safeguard PHI in violation of 45 C.F.R. Section 164.530(c).

18. Health care organizations regulated under HIPAA, like Defendant, may use third-party tracking tools in a limited way to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to vendors (as shown below in Figures 2 through 3). As explained by a statement published by the HHS:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. **For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures**.[7]

19. The Bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, **because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.**[8]

---

[7] HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES (THE "BULLETIN") (EMPHASIS ADDED), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[8] *Id.* (emphasis added).

20. Plaintiff and Class Members face exactly the risks about which the government expresses concern. Defendant's unlawful conduct resulted in third parties intercepting information regarding Plaintiff and Class Members scheduling laser hair removal appointments when logged into their patient portal on the Website.

21. The Bulletin goes on to make clear how broad the government's view of protected information is. It explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, **or any unique identifying code**.[9]

22. Crucially, that paragraph in the government's Bulletin continues:

> All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, **such as IP address** or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus **relates to the individual's past, present, or future health or health care** or payment for care.[10]

23. Then, in July 2022, the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") issued a joint press release warning regulated entities about the privacy and security risks arising from the use of online tracking technologies:

> The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning hospitals and telehealth providers [regulated entities] about the privacy and security risks related to the use of online tracking

[9] *Id.* (emphasis added).

[10] *Id.* (emphasis added).

technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.

"When consumers visit a hospital's [regulated entity's] website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."

"Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a hospital's [regulated entity's] website," said Melanie Fontes Rainer, OCR Director. "OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue."

The two agencies sent the joint letter to approximately 130 [regulated entities] hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.

In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual's personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, **medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment**.[11]

[11] Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, July 20, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking. (emphasis added).

24. Therefore, Defendant's conduct, as described more thoroughly below, is directly contrary to federal law and the clear pronouncements by the FTC and HHS.

B. Google's Advertising Technology

25. Google is one of the most valuable publicly traded companies in the world with a market capitalization of over $1 trillion dollars. Google fancies itself a "tech" company, but Google, at its core, is an advertising company.

26. Google "make[s] money" from "advertising products [that] deliver relevant ads at just the right time," generating "revenues primarily by delivering both performance advertising and brand advertising."[12] In 2020, Google generated $146.9 billion in advertising revenue, which amounted to more than 80 percent of Google's total revenues for the year. Google generated an even higher percentage of its total revenues from advertising in prior years:

Figure 7:

Year	Total Revenue	Ad Revenue	% Ad Revenue
2021	$257.6 billion	$209.5	81.33%
2020	$182.5 billion	$146.9 billion	80.49%
2019	$161.9 billion	$134.8 billion	83.29%
2018	$136.8 billion	$116.5 billion	85.12%

27. Google offers several analytics products, including SDKs and a tracking pixel, which exist solely to help drive ad revenue. For instance, Google's SDK and pixel integrate with Google's advertising offerings, such as Google Ads, Search Ads 360, Google Cloud, and Google Ad Manager, to direct more individuals to use Google's ad network and products increasing Google's overall ad revenue. Products like Google's SDK and its tracking pixel also improve

[12] ALPHABET INC., ANNUAL REPORT (FORM 10-K) (Feb. 2, 2021), available at https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm.

the company's advertising network and capabilities by providing more wholesome profiles and data points on individuals.

28. One of these SDKs and tracking pixels is Google Analytics. Google first launched a version of Google Analytics in 2005 as a tool for website traffic analysis. In 2007, Google launched Google Analytics Synchronous code with new tracking functionality, such as the ability to track commerce transactions. Two years later, Google launched the Google Analytics Asynchronous code, which allowed webpages to load faster and improved data collection and accuracy.

29. Google continued updating its analytics platform, launching Universal Analytics in 2012. Universal Analytics offered new tracking codes and tools that provided more in-depth information about user behavior. Also, Universal Analytics enabled tracking the same user across multiple devices through its addition of the User-ID feature, which "associate[s] a persistent ID for a single user with that user's engagement data from one or more sessions initiated from one or more devices."

30. In 2020, Google launched Google Analytics 4, a platform combining Google Analytics with Firebase to analyze both app and web activity.

31. Since launching Google Analytics, Google has become one of the most popular web analytics platforms on the internet. Indeed, Google had a $62.6 billion increase in advertising revenues in 2021, compared to 2020, after launching its most recent version of Google Analytics.

32. Google touts Google Analytics as a marketing platform that offers "a complete understanding of your customers across devices and platforms."[13] It allows companies and advertisers that utilize it to "understand how your customers interact across your sites and apps, throughout their entire lifestyle," "uncover new insights and anticipate future customer actions with Google's machine learning to get more value out of your data," "take action to optimize marketing performance with integrations across Google's advertising and publisher tools," and "quickly analyze your data and collaborate with an easy-to-use interface and shareable reports."[14]

33. Google Analytics is incorporated into third-party websites and apps, including the Website, by adding a small piece of JavaScript measurement code to each page on the site. This code immediately intercepts a user's interaction with the webpage every time the user visits it, including what pages they visit and what they click on. The code also collects PII, such as IP addresses and device information related to the specific computing device a consumer (or patient) is using to access a website. The device information intercepted by Google includes the patient's operating system, operating system version, browser, language, and screen resolution.

34. Once Google's software code collects the data, it packages the information and sends it to Google Analytics for processing. Google Analytics enables the company or advertiser to customize the processing of the data, such as applying filters. Once the data is processed, it is stored on a Google Analytics database and cannot be changed.

35. After the data has been processed and stored in the database, Google uses this data to generate reports to help analyze the data from the webpages. These include reports on

[13] *Analytics*, GOOGLE, https://marketingplatform.google.com/about/analytics/ (last visited Jan. 10, 2023).

[14] *Id.*

acquisition (e.g., information about where your traffic originates, the methods by which users arrive at your site or app, and the marketing efforts you use to drive traffic), engagement (e.g., measure user engagement by the events and conversion events that users trigger and the web pages and app screens that user visits, and demographics (e.g., classify your users by age, location, language, and gender, along with interests they express through their online browsing and purchase activities).

36. In addition to using the data collected through Google Analytics to provide marketing and analytics services, Google also uses the data collected through Google Analytics to improve its ad targeting capabilities and data points on users.

37. Google Analytics links with Google Ads, so that Google may use the data intercepted by Google Analytics to be utilized for targeted advertising purposes.[15] Such practices were in effect on Defendant's Website at all relevant times.

38. The Website utilizes Google's pixel and SDK. As a result, Google intercepted patients' interactions on the Website, including their PII and PHI. Google received at least "Custom Events" and URLs that disclosed the specific laser hair removal treatment being received by the patient. Google also received additional PII, including the patients' IP address and device information.

39. Google collects vast quantities of consumer data through its tracking technology.

40. Due to the vast network of consumer information held by Google, it is able to match the IP addresses and device information it intercepts and link such information to an individual's specific identity.

41. Google then utilizes such information through targeted advertising.

[15] https://support.google.com/analytics/answer/9379420?hl=en#zippy=%2Cin-this-article

C. Defendant Violates the Privacy Rights of its Customers

42. Laser hair removal treatment is a medical procedure surging in popularity. In 2023, the global laser hair removal industry was valued at over $1 billion.[16]

43. Defendant allows its patients to book appointments through its Website to schedule laser hair removal treatment.

44. Unbeknownst to its patients, Defendant embedded Google's tracking technologies on its Website.

45. After signing into their account, patients can book any of the several laser hair removal treatments offered by Defendant.[17]

46. Defendant provides descriptions of the treatment as well as depictions of the treatment area:

Figure 1:

[16] https://www.fortunebusinessinsights.com/laser-hair-removal-market-103477

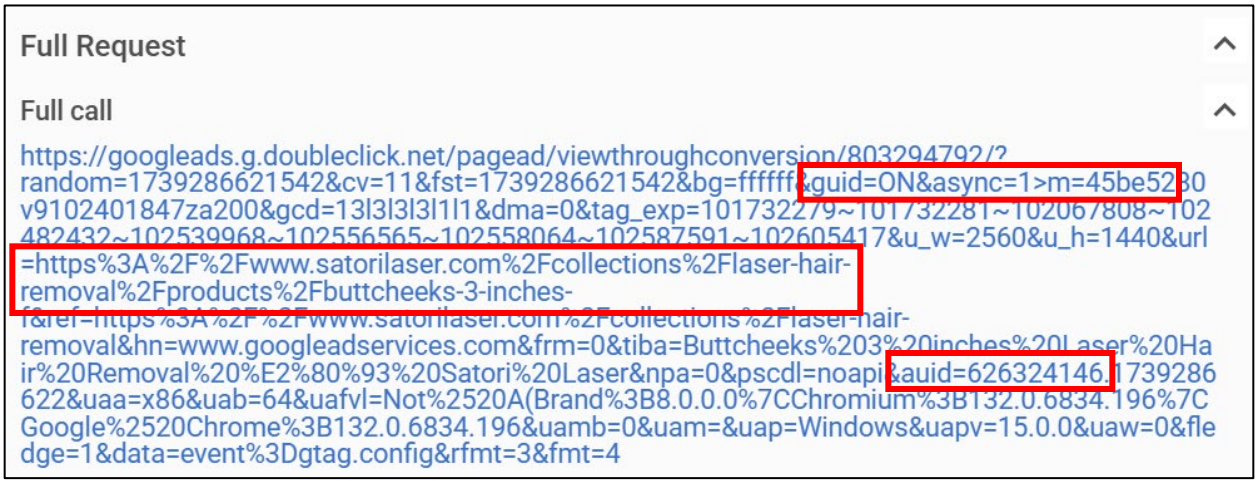
[17] https://www.satorilaser.com/collections/laser-hair-removal

47. When a patient selects a treatment option it is added to their cart, and they begin the checkout process.

48. However, unbeknownst to its patients, Defendant shares their PII and PHI with its advertising partner, Google. The information shared by Defendant allows Google to know the identities of specific individuals as well as information related to the specific laser hair removal treatment they are receiving. This allows these companies, including Defendant, to profit from this information for targeted advertising purposes.

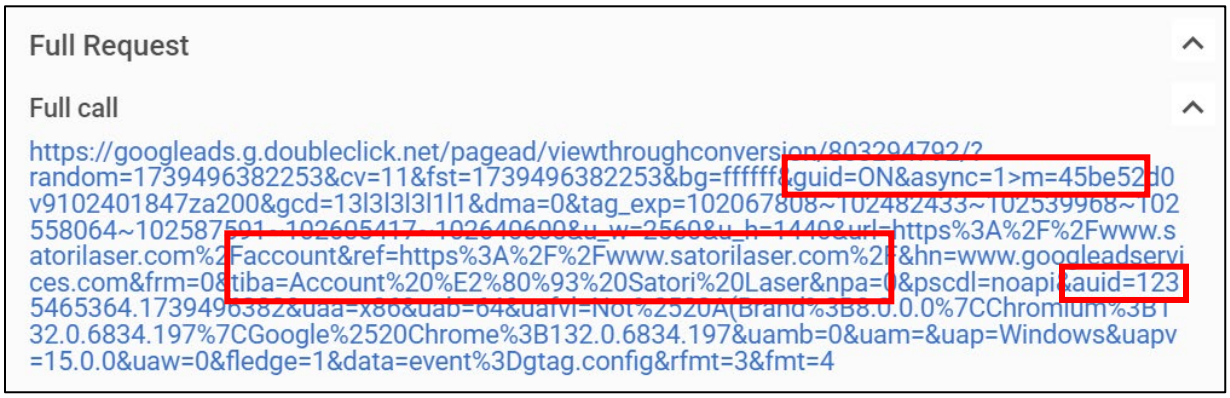
49. For example, when a patient books an appointment for laser hair removal treatment for their buttocks, Defendant assists Google in intercepting the information related to their appointment and the precise treatment locations through both Google Analytics and Google Ads:

Figures 2-3:



50. Defendant assists Google in receiving similar information for every action taken by its patients while they navigate the Website. This includes alerting Google to when its patients have logged into their patient accounts:

Figures 4-5:



51. Defendant further assists Google by disclosing the PII of its patients sufficient for Google to uncover their identities. In both HTTP and HTTPS communications, like Figures 2-5, the patient's IP address is inherently included in every network request. In addition to its patients' IP addresses, Defendant assists Google in intercepting information about their specific devices.

52. As shown above, Plaintiff's communications with Defendant were disclosed by Defendant to these third parties and/or intercepted in transit by the third parties, in real time, via detailed URLs, which contain the medically sensitive information and personally identifiable information entered into the Website.

53. Through its tracking technology, Google intercepts the IP addresses, device information, and User-IDs and links such information to an individual's specific identity.

54. For example, Google utilizes a "cid" or "Client ID," which is a unique identifier utilized by Google and Defendant to "track [a] user['s] interactions across sessions." "Its primary purpose is to uniquely identify users across sessions."[18]

55. Similarly, Google also utilizes the "auid" or "Advertiser User ID," and "guid" or "Globally Unique Identifier," cookies which identify unique users and unique interactions with a website.

56. Defendant sent these identifiers with each patient's "event" data.

[18] https://www.owox.com/blog/use-cases/google-analytics-client-id#:~:text=The%20Client%20ID%20(cid)%20or,unique%20users%20using%20this%20parameter.

57. This disclosed PHI and PII allows Google to know that a specific patient is seeking confidential medical care and the type of medical care being sought, and in addition to permitting Defendant to target those persons with Defendant's ads, Google also then sells that information to marketers who will target Plaintiff and Class members.

58. When patients share their personal information, they expect this information to be kept confidential. Moreover, when consumers seek a specific medical consultation and/or treatment from medical professionals, they also expect this highly sensitive information to be kept confidential.

59. If patients knew that Defendant was sharing their personal information for targeted advertising purposes, they would go to one of its competitors. Through the above-listed third party tracking services, which Defendant used via the software code installed, integrated and embedded into the Website, Defendant disclosed its patients' identities and sensitive medical information.

60. By installing, integrating and embedding the above-listed tracking technologies into the Website, and by directing such installation, integration and embedding, Defendant aided and conspired with the third parties and others to allow those third-party entities to contemporaneously and surreptitiously intercept the Website communications of Defendant's patients without the patients' consent.

61. Defendant engages in this deceptive conduct for its own profit at the expense of its patients. Such disclosures are an invasion of privacy, lead to harassing targeted advertising, and violates federal privacy laws.

CLASS ACTION ALLEGATIONS

62. Plaintiff brings this action on behalf of all persons in the United States who booked an appointment on www.satorilaser.com (the "Class").

63. Excluded from the Class is Defendant, the officers and directors of the Defendant at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which either Defendant has or had a controlling interest.

64. Plaintiff is a member of the Class she seeks to represent.

65. The Class is so numerous that joinder of all members is impractical. Although Plaintiff does not yet know the exact size of the Class, it is believed that there are at least thousands of Class members.

66. The Class is ascertainable because the Class members can be identified by objective criteria – all individuals who booked an appointment on www.satorilaser.com. Individual notice can be provided to Class members "who can be identified through reasonable effort." Fed. R. Civ. P. 23(c)(2)(B).

67. There are numerous questions of law and fact common to the Class, which predominate over any individual actions or issues, including but not limited to:

A. Whether Defendant gave the Class members a reasonable expectation of privacy that their information was not being shared with third parties;

B. Whether Defendant's disclosure of information constitutes a violation of the claims asserted;

C. Whether Plaintiff and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

D. Whether Plaintiff and Class members have sustained damages as a result of Defendant's conduct and if so, what is the appropriate measure of damages or restitution.

68. Plaintiff's claims are typical of the claims of the members of the Class, as all members are similarly affected by Defendant's wrongful conduct. Plaintiff has no interests antagonistic to the interests of the other members of the Class. Plaintiff and all members of the Class have sustained economic injury arising out of Defendant's violations of common and statutory law as alleged herein.

69. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class members she seeks to represent, she has retained counsel competent and experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and her counsel.

70. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and Class members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of

Defendant's liability. Class treatment of the liability issues will ensure that all claims are consistently adjudicated.

71. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CAUSES OF ACTION

COUNT I
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1), *et seq.*

72. Plaintiff incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

73. Plaintiff brings this claim on behalf of herself and members of the Class.

74. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

75. The ECPA protects both sending and the receipt of communications.

76. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

77. The transmission of Plaintiff's PII and PHI to Defendant's Website qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

78. The transmission of PII and PHI between Plaintiff and Class members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate

commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

79. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

80. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

81. The ECPA defines "electronic, mechanical, or other device," as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5).

82. The following instruments constitute "devices" within the meaning of the ECPA:

a. The computer codes and programs Defendant and Google used to track Plaintiff and Class members communications while they were navigating the Website;

b. Plaintiff's and Class members' browsers;

c. Plaintiff's and Class members' mobile devices;

d. Defendant and Google's web and ad servers;

e. The plan Defendant and Google carried out to effectuate the tracking and interception of Plaintiff's and Class members' communications while they were using a web browser to navigate the Website.

83. Plaintiff and Class members' interactions with Defendant's Website are electronic communications under the ECPA.

84. By utilizing and embedding the tracking technology provided by Google on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class members in violation of 18 U.S.C. § 2511(1)(a).

85. Specifically, Defendant intercepted—in real time—Plaintiff's and Class members' electronic communications via the tracking technology provided by Google on its Website, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' PII and PHI to third parties, such as Google.

86. Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class members regarding PII and PHI, including their identities and information related to their laser hair removal appointments. This confidential information is then monetized for targeted advertising purposes, among other things.

87. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class members' electronic communications to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

88. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

89. Defendant intentionally intercepted the contents of Plaintiff's and Class members' electronic communications for the purpose of committing a criminal or tortious act in violation

of the Constitution or laws of the United States or of any state, namely, invasion of privacy, among others.

90. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information ("IIHI") to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[19]

91. Plaintiff's information that Defendant disclosed to Google qualifies as IIHI, and Defendant violated Plaintiff's and Class members' expectations of privacy. Such conduct constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d-6. Defendant used the electronic communications to increase its profit margins. Defendant specifically used the tracking technology provided by Google to track and utilize Plaintiff's and Class members' PII and PHI for financial gain.

92. Defendant was not acting under the color of law to intercept Plaintiff's and Class members' wire or electronic communications.

[19] 42 U.S.C. § 1320d-6.

93. Plaintiff and Class members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class members' privacy. Plaintiff and Class members, all of whom are patients of Defendant, had a reasonable expectation that Defendant would not redirect their communications to Google without their knowledge or consent.

94. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq*.

95. As a result of each and every violation thereof, on behalf of herself and the Class, Plaintiff seeks statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510, et seq. under 18 U.S.C. § 2520.

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

a. Determining that this action is a proper class action;

b. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the Class and naming Plaintiff's attorneys as Class Counsel to represent the Class;

c. For an order declaring that Defendant's conduct violates the statutes referenced herein;

d. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

e. Award compensatory damages, including statutory damages where available, to Plaintiff and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;

f. Ordering Defendant to disgorge revenues and profits wrongfully obtained;

g. For prejudgment interest on all amounts awarded;

h. For injunctive relief ordering Defendant to immediately cease its illegal conduct;

i. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit; and

j. Grant Plaintiff and the Class members such further relief as the Court deems appropriate.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all claims so triable in this action.

Dated: February 27, 2025

Respectfully submitted,

By: */s/ Alec Leslie*

BURSOR & FISHER, P.A.
Alec M. Leslie
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: aleslie@bursor.com

BURSOR & FISHER, P.A.
Stephen A. Beck (*pro hac vice* forthcoming)
701 Brickell Ave., Suite 2100
Miami, FL 33131
Tel: (305) 330-5512
Fax: (305) 676-9006
E-Mail: sbeck@bursor.com

Attorneys for Plaintiff